ABSTRACT OF THE DISCLOSURE

Methods and systems in accordance with the present invention efficiently validate digital certificates by answering Online Certificate Status Protocol ("OCSP") requests without Certificate Revocation Lists ("CRL"). During validation of digital certificates, these methods and systems speed transmission, reduce required bandwidth and reduce required data storage by eliminating the need for the transmission of lengthy CRLs from a Certificate Authority ("CA") when verifying a digital certificate from a client. In one implementation, they send a Lightweight Directory Access Protocol ("LDAP") database query to a CA directory server to determine and pinpoint the existence of a valid digital certificate and check its validity without receiving a long list of data, such as a CRL, from a CA. The CA directory server returns the query result, and the database query in the CA directory server is performed faster than using an entire CRL, and furthermore, the transmission of the database query result is a small piece of information and does not require the large amounts of data transmission bandwidth and storage as required with transmitting CRL's.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000